Justin Lew

Cybersecurity Compliance Checklist

Framework Alignment: This checklist aligns with NIST Cybersecurity Framework (NIST CSF), CIS Controls, and ISO 27001.

---

1. Data Protection & Privacy

✅ Identify and classify sensitive data based on confidentiality and regulatory requirements.

✅ Implement data encryption for storage (AES-256) and transmission (TLS 1.2/1.3).

✅ Establish a data retention and disposal policy aligned with compliance mandates.

✅ Conduct regular data protection impact assessments (DPIAs) and risk assessments.

✅ Ensure compliance with GDPR, HIPAA, or other applicable regulatory frameworks.

✅ Deploy access controls using identity and access management (IAM) solutions.

✅ Implement secure backup and disaster recovery solutions with periodic testing.

✅ Monitor and log data access activities using SIEM solutions.

2. Access Control & Identity Management

✅ Enforce multi-factor authentication (MFA) for all privileged accounts and remote access.

✅ Implement role-based access control (RBAC) and attribute-based access control (ABAC).

✅ Regularly review and update user permissions based on job function changes.

✅ Ensure secure authentication mechanisms (e.g., Single Sign-On, strong password policies).

✅ Remove inactive user accounts within a defined timeframe.

✅ Implement least privilege and zero trust principles for network segmentation.

✅ Monitor and analyze unauthorized access attempts with anomaly detection tools.

3. Incident Response & Monitoring

✅ Develop and maintain a Computer Security Incident Response Plan (CSIRP) aligned with NIST 800-61.

✅ Establish an incident reporting and escalation process with defined SLAs.

✅ Conduct regular incident response tabletop exercises and penetration tests.

✅ Define roles and responsibilities in a RACI matrix.

✅ Implement continuous security monitoring with SIEM, IDS/IPS, and SOAR platforms.

✅ Maintain up-to-date threat intelligence feeds integrated into detection tools.

✅ Document and analyze security incidents for continuous improvement and response tuning.

4. Vulnerability & Patch Management

✅ Perform regular vulnerability scans and penetration testing using industry-standard tools (e.g., Nessus, Qualys).

✅ Maintain an up-to-date asset inventory with criticality ratings.

✅ Prioritize and remediate critical vulnerabilities based on risk assessment.

✅ Deploy patches and updates in a timely manner with automated deployment where possible.

✅ Monitor security advisories for emerging threats and zero-day vulnerabilities.

✅ Implement endpoint detection and response (EDR) solutions to detect and mitigate threats.

✅ Maintain secure software development lifecycle (SDLC) processes, including secure coding practices.

5. Security Awareness & Training

✅ Conduct regular security awareness training, including phishing and social engineering simulations.

✅ Provide specialized training for employees handling sensitive data or critical systems.

✅ Ensure employees understand and acknowledge data handling and security policies annually.

✅ Establish a secure remote work policy with guidelines for endpoint security.

✅ Provide incident reporting training to ensure quick response to potential threats.

✅ Regularly update training materials based on emerging threat landscapes and past incidents.

6. Compliance Audit & Reporting

✅ Conduct regular cybersecurity audits and risk assessments aligned with compliance standards.

✅ Maintain up-to-date documentation of security policies, standards, and procedures.

✅ Implement Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to measure compliance effectiveness.

✅ Align security controls with business objectives and regulatory requirements.

✅ Document audit findings and remediation steps with prioritization based on risk impact.

✅ Maintain a formal risk register and track remediation progress.

✅ Engage third-party auditors to validate security compliance where required.

Justin Lew

Mock Compliance Audit Report

Organization: ExampleCorp Ltd.
Audit Date: (Date)
Compliance Framework: NIST CSF, CIS Controls, ISO 27001
Lead Auditor: (Auditor Name)

Audit Summary

- **Overall Compliance Score:** 85%
- **Key Findings:**
  - Strong access controls and identity management practices.
  - Well-documented and tested incident response plan.
  - Patch management process needs improvement, particularly on legacy systems.
  - Data encryption policies require updates to align with current compliance standards.
- **Recommendations:**
  - Implement automated patch management solutions to reduce risk exposure.
  - Enhance security awareness training frequency and phishing simulations.
  - Conduct additional penetration testing for third-party integrations and cloud environments.

Compliance Scorecard

Compliance Area	Score	Notes
Data Protection	90%	Minor gaps in encryption policy.
Access Control	95%	Strong implementation of RBAC & MFA.
Incident Response	85%	Requires additional testing exercises.
Vulnerability Management	75%	Delays in patch deployment.
Security Awareness Training	80%	Needs more frequent simulations.
Compliance Reporting	88%	Well-documented policies.

Conclusion

ExampleCorp Ltd. has a solid cybersecurity program in place, but there are areas that need work, such as patch management and security awareness training. Addressing these issues will help improve overall compliance and make the organization more resilient against cyber threats.